

Appl. No. 09/646,640
Amdt. dated Dec. 14, 2004
Reply to Office Action of July 14, 2004

Amendments to the Claims:

- 1 1. (cancelled).

- 1 2. (currently amended) ~~Protection~~ The protection method according to claim ~~1~~ 2,
2 ~~characterized in that~~ wherein a randomly transformed data element is a key (K1,
3 K2, K3, K4, K5).

- 1 3. (currently amended) ~~Protection~~ The protection method according to claim ~~1~~ 2,
2 ~~characterized in that~~ wherein a randomly transformed data element is a message
3 block (M, M0, M1, M2, M3).

- 1 4. (currently amended) ~~Protection~~ The protection method according to claim ~~1~~ 2,
2 ~~characterized in that~~ wherein a randomly transformed data element is a message
3 block associated with a key by a logical operator of the exclusive-OR type (R1,
4 R2, R3, R4, R5).

- 1 5. (currently amended) ~~Protection~~ The protection method according to claim ~~1~~ 2,
2 ~~characterized in that~~ wherein the cryptographic algorithm for executing
3 operations for processing data (M, M0, M1, M2, M3, K1, K2, K3, K4, K5, R1,
4 R2, R3, R4, R5) comprises a group of operations (270) executed repeatedly.

- 1 6. (currently amended) ~~Protection~~ The protection method according to claim 5,
2 ~~characterized in that~~ wherein the random transformation step is a step that
3 precedes the group of operations (270) executed repeatedly and in that the
4 inverse transformation step is a step that follows said group of operations (270).

Appl. No. 09/646,640
Amdt. dated Dec. 14, 2004
Reply to Office Action of July 14, 2004

1 7. (currently amended) ~~Protection~~ The protection method according to claim 1 2,
2 ~~characterized in that~~ further comprising a step for randomly modifying the order
3 of execution of the operations of the group of operations (270).

1 8. (currently amended) ~~Protection~~ The protection method according to claim 1 2,
2 ~~characterized in that~~ wherein the cryptographic algorithm is the DATA
3 ENCRYPTION STANDARD type.

1 9. (new) Data protection method for protecting data elements processed by a
2 microprocessor in a chip card from discovery by analysis of the microprocessor's
3 electric power consumption, said method using a cryptographic algorithm for
4 executing operations for processing said data elements so as to generate
5 encrypted information, said method comprising:
6 random transformation of at least one of the data elements by associating said
7 at least one of the data elements with a random number generated by
8 an unpredictable number generator, by means of a logical operator of
9 the exclusive-OR type, and
10 after this random transformation step, an inverse transformation step such
11 that the encrypted information is unchanged by these transformation
12 steps.

1 10. (new) Data protection method for protecting data elements processed by a
2 microprocessor in a chip card from discovery by analysis of the microprocessor's
3 electric power consumption, said method using a cryptographic algorithm for
4 executing operations for processing said data elements so as to generate
5 encrypted information, said method comprising:

Appl. No. 09/646,640
Amdt. dated Dec. 14, 2004
Reply to Office Action of July 14, 2004

6 randomly modifying the order of execution of operations from one cycle to
7 another, a cycle being a complete execution cycle of the algorithm or
8 an intermediate cycle of a group of operations, said operations being
9 operations whose order of execution relative to the others does not
10 affect the result.

1 11. (new) The protection method according to claim 10, wherein the modified order
2 of execution of operations include permutation of bits of a message block before
3 permutation of bits of a key, and vice versa.

1 12. (new) The protection method according to claim 10, wherein the modified order
2 of execution of operations include modifying the order of processing quartets
3 making up a data element.

1 13. (new) The protection method according to claim 10, wherein the modification of
2 the order of execution of operations is random.